ABSTRACT

A method and system for preserving the integrity of a negotiation that includes providing an architecture which includes a center A, and a plurality of users B.sub.1, B.sub.2,..., B.sub.n. each user B.sub.i generates an input X.sub.i, which is input to the center A. The center A computes and publishes a function F(X.sub.1,X.sub.2,...,X.sub.n) based on the input messages it receives. Each user B.sub.i (1<= i<= n) communicates with the center A, exclusively. Center A publishes additional information which lets each of the users verify that F was computed correctly, and prevents a coalition of any one subset of the users from learning anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, or information about the inputs of other users.